STATE OF CONNECTICUT

QUI TRANSTULIT SUSTINET

General Assembly

File No. 642

January Session, 2017

Substitute House Bill No. 7304

House of Representatives, April 18, 2017

The Committee on Judiciary reported through REP. TONG of the 147th Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

AN ACT CONCERNING COMPUTER EXTORTION BY USE OF RANSOMWARE.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1   Section 1. (NEW) (*Effective October 1, 2017*) (a) A person is guilty of
2   computer extortion by use of ransomware, when such person (1)
3   introduces ransomware into any computer, computer system or
4   computer network, and (2) demands payment of money or other
5   consideration to remove the ransomware, restore access to the
6   computer, computer system, computer network or data contained on
7   such computer, computer system or computer network, or otherwise
8   remediate the impact of the ransomware.

9   (b) Computer extortion by use of ransomware is a class E felony.

10   (c) For purposes of this section, "ransomware" means any computer
11   contaminant or lock placed or introduced without authorization into a
12   computer, computer system or computer network that restricts access
13   by an authorized person to the computer, computer system, computer

14   network, or any data held by the computer, computer system or
15   computer network, but does not include authentication required to
16   upgrade or access purchased content or the blocking of access to
17   subscription content in the case of nonpayment for such access, and
18   "computer contaminant" means any set of computer instructions that
19   are designed to modify, damage, destroy, record or transmit data held
20   by a computer, computer system or computer network without the
21   intent or permission of the owner of the data.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2017*	New section

JUD   *Joint Favorable Subst.*

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 18 $	FY 19 $
Correction, Dept.; Judicial Dept. (Probation)	GF - Potential Cost	See Below	See Below
Resources of the General Fund	GF - Potential Revenue Gain	See Below	See Below

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill creates a new felony for computer extortion involving ransomware and results in a potential cost for incarceration/probation and potential revenue from new offense violations. As this is a new offense, the impact of the bill is unknown. To the extent that offenders are prosecuted for new offense, potential costs for incarceration or probation supervision in the community, or judicial revenue would result. On average, it costs the state $7,260 (including benefits) to supervise an inmate in the community as opposed to $61,320 (including benefits) to incarcerate an offender.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to the number of violations.

OLR Bill Analysis

sHB-7304

AN ACT CONCERNING COMPUTER EXTORTION BY USE OF RANSOMWARE.

SUMMARY

This bill creates a specific class E felony offense for computer extortion involving ransomware. The punishable actions include introducing ransomware into a computer, computer system, or computer network and demanding payment to (1) remove the ransomware; (2) restore access to the computer, system, or network or data contained therein; or (3) otherwise remediate the ransomware's impact. A class E felony is punishable by up to three years in prison, up to a $3,500 fine, or both. Individuals who commit this crime may also be charged with certain other computer crimes, computer-related offenses, and extortion under existing law (see BACKGROUND).

The bill defines "ransomware" as any computer contaminant or lock placed or introduced without authorization into a computer, system, or network, that restricts the authorized person's access to the affected computer, system, network, or data contained therein. It does not include (1) authentication required to upgrade or access purchased content or (2) blocking access to subscription content in the case of nonpayment.

A "computer contaminant" is any set of computer instructions designed to modify, damage, destroy, record, or transmit data held by a computer, system, or network without the data owner's intent or permission.

EFFECTIVE DATE: October 1, 2017

BACKGROUND

Computer Crimes

The law designates various actions as computer crimes, including unauthorized use of a computer or computer network with the intent to (1) temporarily or permanently remove, or otherwise disable computer programs, software, or data or (2) cause a computer to malfunction regardless how long the malfunction persists. Any such action is punishable as (1) a class A or B misdemeanor depending on the amount of property damage the action causes or (2) a class D felony if the action was malicious and caused more than $2,500 in property damage (CGS § 53-451).

Computer-Related Offenses

The law designates various computer-related offenses, including (1) accessing a computer system without authorization, (2) stealing or interrupting computer services, (3) misusing computer system information, and (4) destroying computer equipment. The penalties range from a class B misdemeanor to a class B felony depending on the amount of damage to, or value of, the property or computer services (CGS §§ 53a-250 *et seq.*).

Extortion

By law, people obtain property by extortion when they compel or induce someone to deliver property to them or another person by instilling fear that, if the property is not delivered, they will take certain actions, including damaging the property or inflicting other harm. Obtaining property by extortion is 1st degree larceny, a class B felony, punishable by up to 20 years in prison, up to a $15,000 fine, or both (CGS §§ 53a-119, 53a-122).

COMMITTEE ACTION

Judiciary Committee

Joint Favorable Substitute
Yea   39   Nay   0   (03/31/2017)